29. (NEW) A self-authenticating document having critical document data, comprising:

a first digital signature including a first digest of said critical document data;

a second digital signature including a second digest of said critical document data and a personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said first and second digital signatures, wherein said first digital signature, said second digital signature, and said public key certificate are stored on said self-authenticating document.

30. (NEW) The self-authenticating document of claim 29, wherein said first digital signature, said second digital signature, and said public key certificate are stored in machine-readable format on said self-authenticating document.

a1

31. (NEW) The self-authenticating document of claim 30, wherein said critical document data includes data contained in a magnetic ink character recognition (MICR) code line on said self-authenticating document.

32. (NEW) The self-authenticating document of claim 31, wherein said critical document data further includes ASCII text from said document.

33 (NEW) The self-authenticating document of claim 32, wherein said ASCII text is the account name and address printed on said self-authenticating document.

34 (NEW) The self-authenticating document of claim 31, wherein said document is a personal value document.

35. (NEW) The self-authenticating document of claim 34, wherein said personal value document is a personal check.

36. (NEW) The self-authenticating document of claim 34, wherein said personal value document is selected from the group consisting of: an identification card, a Social Security card, a driver's license, a birth certificate, a credit card, a voter's registration card, and a passport.

37. (NEW) The self-authenticating document of claim 30, wherein said machine-readable format is a bar code.

38. (NEW) The self-authenticating document of claim 37, wherein said bar code format is PDF 417.

a'

39. (NEW) The self-authenticating document of claim 37, wherein said bar code comprises a plurality of data fields.

40. (NEW) The self-authenticating document of claim 39, wherein said bar code includes:

a first data field including data representing the number of bytes of data in said bar code;

a second data field including said public key certificate;

a third data field including data representing the number of bytes of data in said critical document data; and,

a fourth data field including said critical document data.

41. (NEW) The self-authenticating document of claim 40, wherein said bar code further includes a fifth data field including said second digital signature.

a1

42. (NEW) The self-authenticating document of claim 40, wherein said bar code further includes a sixth data field including said first digital signature.

43. (NEW) A self-authenticating document having critical document data, comprising:

a digital signature including a digest of said critical document data and personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said digital signature, wherein said digital signature and said public key certificate are stored on said self-authenticating document.

44. (NEW) The self-authenticating document of claim 43, wherein said digital signature and said public key certificate are stored in machine-readable format on said self-authenticating document.

45. (NEW) The self-authenticating document of claim 44, wherein said document is a personal value document.

46. (NEW) The self-authenticating document of claim 45, wherein said personal value document is a personal check.

47. (NEW) The self-authenticating document of claim 45, wherein said personal value document is selected from the group consisting of: an identification card, a Social Security card, a driver's license, a birth certificate, a credit card, a voter's registration card, and a passport.

48. (NEW) The self-authenticating document of claim 45, wherein said critical document data includes data contained in a magnetic ink character recognition (MICR) code line on said self-authenticating document.

49. (NEW) The self-authenticating document of claim 48, wherein said critical document data further includes ASCII text from said self-authenticating document.

50. (NEW) The self-authenticating document of claim 49, wherein said ASCII text is the account name and address printed on said self-authenticating document.

51. (NEW) The self-authenticating document of claim 44, wherein said machine-readable format is a two-dimensional bar code.

52. (NEW) The self-authenticating document of claim 51, wherein said two-dimensional bar code format is PDF 417.

53. (NEW) The self-authenticating document of claim 51, wherein said two-dimensional bar code comprises a plurality of two-byte data fields.

54. (NEW) The self-authenticating document of claim 53, wherein said two-dimensional bar code includes:

a first data field including data representing the number of bytes of data in said bar code;

a second data field including said public key certificate;

a third data field including data representing the number of bytes of data in said critical document data; and,

a fourth data field including said critical document data.

55. (NEW) The self-authenticating document of claim 54, wherein said two-dimensional bar code further includes a fifth data field including said digital signature.

56. (NEW) The self-authenticating document of claim 43, wherein said personal identification number is a four digit number comprising four bytes of data.

57. (NEW) The self-authenticating document of claim 43, wherein said personal identification number is selected by the owner of said personal value document.

58. (NEW) The self-authenticating document of claim 43, wherein a third party responsible for printing said personal value document selects said personal identification number.

59. (NEW) The self-authenticating document of claim 43, wherein a third party responsible for issuing said personal value document selects said personal identification number.

60. (NEW) The self-authenticating document of claim 43, wherein the digital signature algorithm used to create said digest of said digital signature is a public key cryptographic algorithm.

61. (NEW) The self-authenticating document of claim 60, wherein said digital signature algorithm is an elliptic curve digital signature algorithm (ECDSA).

62. (NEW) The self-authenticating document of claim 43, wherein said public key certificate further includes identity information of the owner of said authentic public key and a digital signature of said authentic public key and said owner identity information, and wherein said digital signature is issued by a third party.

63. (NEW) The self-authenticating document of claim 62, wherein said third-party digital signature is created using the elliptic curve digital signature algorithm (ECDSA).

64. (NEW) The self-authenticating document of claim 63, wherein said ECDSA algorithm includes a first group of shared parameters for implementing said digital signature.

65. (NEW) The self-authenticating document of claim 64, wherein said ECDSA used to create said third-party digital signature includes a second group of shared parameters for implementing said third-party digital signature.

a'

66. (NEW) The self-authenticating document of claim 65, wherein said first group of shared parameters is the same as said second group of shared parameters.

67. (NEW) The self-authenticating document of claim 65, wherein said first group of shared parameters is different from said second group of shared parameters.

68. (NEW) The self-authenticating document of claim 65, wherein said first and second groups of shared parameters is distributed to a community of users of said self-authenticating document.

69. (NEW) The self-authenticating document of claim 68, wherein said third party is a certificate authority.

70. (NEW) The self-authenticating document of claim 68, wherein said community of users includes a party responsible for issuing said self-authenticating document, a party responsible for printing said self-authenticating document, and said certificate authority.

71. (NEW) The self-authenticating document of claim 70, wherein said community of users further includes an owner of said self-authenticating document.

72. (NEW) The self-authenticating document of claim 43, wherein said public key certificate is affixed to said self-authenticating document by a third party responsible for printing said self-authenticating document.

a'

73. (NEW) The self-authenticating document of claim 43, wherein said public key certificate is affixed to said self-authenticating document by a third party responsible for issuing said public key certificate.

74. (NEW) The self-authenticating document of claim 73, wherein said third party is a certificate authority.

75. (NEW) A personal value document, comprising:

a first digital signature including a first digest of critical document data, said critical document data including data contained in a magnetic ink character recognition (MICR) code line on said personal value document;

a second digital signature including a second digest of said critical document data and a personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said first and second digital signatures, wherein said first digital signature, said second digital signature, and said public key certificate are stored in a bar code format on said personal value document.

76. (NEW) The personal value document of claim 75, wherein said personal value document is a personal check.

77. (NEW) The personal value document of claim 75, wherein said critical document data further includes ASCII text from said personal check.

78. (NEW) The personal value document of claim 77, wherein said ASCII text is the account name and address printed on said personal check.

79. (NEW) The personal value document of claim 77, wherein said bar code comprises a plurality of date fields, including:

a first data field including data representing the number of bytes of data in said bar code;

a second data field including said public key certificate;

a third data field including data representing the number of bytes of data in said critical document data; and,

a fourth data field including said critical document data.

80. (NEW) The personal value document of claim 79, wherein said two-dimensional bar code further includes:

a fifth data field including said second digital signature; and,

a sixth data field including said first digital signature.

81. (NEW) The personal value document of claim 75, wherein the digital signature algorithm used to create said first digest of said first digital signature and said second digest of said second digital signature is a public key cryptographic algorithm.

82. (NEW) The personal value document of claim 81, wherein the digital signature algorithm used to create said first digest is the elliptic curve digital signature algorithm (ECDSA).

83. (NEW) The personal value document of claim 82, wherein the digital signature algorithm used to create said second digest is the elliptic curve digital signature algorithm (ECDSA).

84. (NEW) The personal value document of claim 75, wherein said personal identification number is selected by the owner of said personal value document.

85. (NEW) The personal value document of claim 83, wherein said public key certificate further includes identity information of the owner of said authentic public key and a digital signature of said authentic public key and said owner identity information, and wherein said digital signature is issued by a certificate authority.

86. (NEW) The personal value document of claim 85, wherein said ECDSA used to create said first and second digital signatures respectively includes a first group of shared parameters for implementing said first and second digital signatures, and wherein said ECDSA used to create said certificate authority digital signature includes a second group of shared parameters for implementing said certificate authority digital signature.

87. (NEW) The personal value document of claim 86, wherein said first group of shared parameters is the same as said second group of shared parameters.

a1

88. (NEW) The personal value document of claim 86, wherein said first group of shared parameters is different from said second group of shared parameters.

89. (NEW) The personal value document of claim 86, wherein said first and second groups of shared parameters is distributed to a community of users of said personal value document.

90. (NEW) The personal value document of claim 89, wherein said community of users includes a party responsible for issuing said personal value document, a party responsible for printing said personal value document, and said certificate authority.

91. (NEW) The personal value document of claim 90, wherein said community of users further includes an owner of said personal value document.

92. (NEW) The personal value document of claim 75, wherein said first and second digital signatures, and said public key certificate are affixed to said personal value document by a third party responsible for printing said personal value document.

93. (NEW) A self-authenticating document having critical document data, comprising:

a digital signature including a digest of said critical document data; and,

a public key certificate including an authentic public key for validating said digital signature, wherein said digital signature and said public key certificate are stored in machine-readable format on said self-authenticating document.

94. (NEW) The self-authenticating document of claim 93, wherein said critical document data includes data contained in a magnetic ink character recognition (MICR) code line on said self-authenticating document.

95. (NEW) The self-authenticating document of claim 94, wherein said critical document data further includes ASCII text from said self-authenticating document.

96. (NEW) The self-authenticating document of claim 94, wherein said self-authenticating document is a commercial value document.

97. (NEW) The self-authenticating document of claim 96, wherein said commercial value document is selected from the group consisting of: a bank check, a business check, tickets, gift certificates, titles, negotiable letters of credit, and currency.

98. (NEW) The self-authenticating document of claim 96, wherein said machine-readable format is a bar code, said bar code comprising a plurality of data fields.

99. (NEW) The self-authenticating document of claim 98, wherein said code includes:

a first data field including data representing the number of bytes of data in said bar code;

a second data field including said public key certificate;

a' a third data field including data representing the number of bytes of data in said critical document data;

a fourth data field including said critical document data; and,

a fifth data field including said digital signature.

100. (NEW) A method for creating a self-authenticating document having critical document data, said critical document data including machine-readable data printed on said self-authenticating document, said method comprising the steps of:

creating a first digital signature by signing said critical document data with a digital signature algorithm;

creating a second digital signature by signing said critical document data critical document data and a personal identification number (PIN) with said digital signature algorithm;

retrieving a public key certificate including an authentic public key for validating said first and second digital signatures; and,

affixing said first and second digital signatures and said public key certificate to said self-authenticating document in a machine-readable format.

101. (NEW) The method of claim 100, wherein said critical document data includes ASCII text from said self-authenticating document, and further comprising the step of:

storing said ASCII text in a machine-readable format on said self-authenticating document prior to said first digital signature creating step.

102. (NEW) The method of claim 100, further comprising the steps of:

selecting a group of shared parameters corresponding to said digital signature algorithm for implementing said first and second digital signatures;

generating a public key and a private key using said shared parameters;

certifying said public key via a certificate authority,

wherein said selecting, generating and certifying steps are carried out prior to said first digital signature creation step.

103. (NEW) The method of claim 100, wherein said step of creating said first digital signature includes the substeps of:

generating a public key and a private key using said digital signature algorithm;

assembling said critical document data from said self-authenticating document; and,

applying said private key generated by said digital signature algorithm to said critical document data to create said first digital signature.

104. (NEW) The method of claim 103, wherein said step of creating said second digital signature includes the substeps of:

generating said personal identification number (PIN);

appending said personal identification number (PIN) to said critical document data to create an authenticatable data string; and,

applying said private key generated by said digital signature algorithm to said authenticatable data string to create said second digital signature.

105. (NEW) The method of claim 104, wherein said digital signature algorithm is an elliptic curve digital signature algorithm (ECDSA).

106. (NEW) The method of claim 104, wherein said step of affixing said first and second digital signatures to said self-authenticating document includes the substeps of:

assembling a k– byte data string, wherein k includes the number of bytes in said critical document data, said authenticatable data, and said public key certificate; and,

generating a machine-readable data string from said k– byte data string.

107. (NEW) The method of claim 106, further comprising the step of calculating the total amount of bytes of data, k, including said critical document data, said authenticatable data string, and said public key certificate, prior to said k– byte data string assembling step.

108. (NEW) The method of claim 107, wherein said first and second digital signatures and said public key certificate are affixed in bar-code format to said self-authenticating document, and wherein said step of generating said machine readable data string comprises the substep of converting said k– byte data string into bar code print data.

109. (NEW) A method for creating a self-authenticating document having critical document data, said critical document data including machine-readable data printed on said self-authenticating document, said method comprising the steps of:

creating a first digital signature by signing said critical document data with a digital signature algorithm;

creating a second digital signature by signing said critical document data and a personal identification number (PIN) with said digital signature algorithm;

retrieving a public key certificate including an authentic public key for validating said first and second digital signatures;

determining whether said second digital signature is to be affixed to said self-authenticating document;

determining whether said first digital signature is to be affixed to said self-authenticating document;

affixing said public key certificate and at least one of said first digital signature and said second digital signature to said self-authenticating document in machine-readable code, based on the results of the second digital signature and first digital signature determining steps.

110. (NEW) The method of claim 109, wherein said critical document data includes ASCII text from said self-authenticating document, and further comprising the step of:

storing said ASCII text in a machine-readable format on said self-authenticating document prior to said first digital signature creating step.

111. (NEW) The method of claim 109, further comprising the steps of:

selecting a group of shared parameters corresponding to said digital signature algorithm for implementing said at least one of said first and second digital signatures;

generating a public key and a private key using said shared parameters;

certifying said public key via a certificate authority,

wherein said selecting, generating and certifying steps are carried out prior to said first digital signature creation step.

112. (NEW) The method of claim 109, said step of creating said first digital signature includes the substeps of:

generating a public key and a private key using said digital signature algorithm;

assembling said critical document data said self-authenticating document; and,

applying said private key generated by said digital signature algorithm to said critical document data to create said first digital signature.

113. (NEW) The method of claim 112, said step of creating said second digital signature includes the substeps of:

generating said personal identification number (PIN);

appending said personal identification number (PIN) to said critical document data to create an authenticatable data string; and,

applying said private key generated by said digital signature algorithm to said authenticatable data string to create said second digital signature.

114. (NEW) The method of claim 109, wherein said digital signature algorithm is an elliptic curve digital signature algorithm (ECDSA).

115. (NEW) The method of claim 109, wherein if it is determined that said first digital signature is to be affixed to said self-authenticating document, said step of affixing said first digital signature to said self-authenticating document includes the substeps of:

assembling a k– byte data string, wherein k includes the number of bytes in said critical document data; and,

generating a machine-readable data string from said k– byte data string.

116. (NEW) The method of claim 109, wherein if it is determined that said second digital signature is to be affixed to said self-authenticating document, said step of affixing said second digital signature to said self-authenticating document includes the substeps of:

assembling a k– byte data string, wherein k includes the number of bytes in said authenticatable data string; and,

generating a machine-readable data string from said k– byte data string.

117. (NEW) The method of claim 109, wherein if it is determined that said first and said second digital signatures are to be affixed to said self-authenticating document, said step of affixing said first and second digital signatures to said self-authenticating document includes the substeps of:

assembling a k– byte data string, wherein k includes the number of bytes in said critical document data and said authenticatable data string; and,

generating a machine-readable data string from said k– byte data string.

118. (NEW) The method of claim 117, further comprising the step of calculating the total amount of bytes of data, k, in said critical document data and said authenticatable data string, prior to said k– byte data string assembling step.

119. (NEW) A method of authenticating a self-authenticating document, comprising the steps of:

processing machine-readable data on said self-authenticating document to obtain digital signature data and a public key certificate;

processing said public key certificate to obtain public key certificate data including an authentic public key;

assembling critical document data from said self-authenticating document, wherein said critical document data includes at least magnetic ink character recognition (MICR) data printed on said self-authenticating document;

a' determining whether an authentic personal identification number (PIN) is available for appending to said critical document data;

wherein, if said authentic PIN is available;

appending said authentic PIN to said critical document data to create an authenticatable data string; and,

applying said authentic public key to said digital signature data to validate said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

120. (NEW) The authenticating method of claim 119, wherein said self-authenticating document is a personal check, and wherein said critical document data includes ASCII text printed on said personal check.

121. (NEW) The authenticating method of claim 119, further comprising the steps of:

determining whether a first digital signature is present in said digital signature data, if it is determined that said authentic personal identification number (PIN) is not available;

applying said authentic public key to said digital signature data to validate said critical document data, wherein said self-authenticating document is authenticated if said critical document data is validated.

122. (NEW) The authenticating method of claim 121, wherein if it is determined that said authentic PIN is not available and that said first digital signature is not present in said digital signature data, further comprising the steps of:

determining whether a second digital signature is present in said digital signature data, and,

if said second digital signature is present;

generating a plurality of PINs;

appending each of said plurality of PINs to said critical document data to create a plurality of verifiable data strings; and,

applying said authentic public key to said second digital signature in order to validate one of said verifiable data strings as said authenticatable data string and to authenticate said self-authenticating document.

123. (NEW) The authenticating method of claim 122, wherein said step of generating PINs is carried out in a document reading system executing a PIN-generating algorithm.

124. (NEW) The authenticating method of claim 121, wherein said machine-readable data is bar-code data, said machine-readable data processing step including the substeps of:

retrieving said bar code data from said self-authenticating document; and,

parsing data fields in said bar code data to obtain at least said public key certificate, said digital signature data, and k_s where k_s is the total number of bytes in said bar code data.

125. (NEW) The authenticating method of claim 121, wherein said public key certificate data processing step includes the substeps of:

validating said public key certificate with a third-party public key; and,

parsing said public key certificate to obtain said authentic public key;

126. (NEW) The authenticating method of claim 125, wherein said public key certificate includes a third-party digital signature, and wherein said public key certificate validating step further comprises the substep of applying said third-party public key to said third-party digital signature.

127. (NEW) The authenticating method of claim 125, wherein said third party is a certificate authority.

128. (NEW) The authenticating method of claim 125, wherein said public key certificate is comprised of m bytes, and wherein said public key certificate parsing substep includes the further substeps of:

retrieving at least a first byte, c_1, of said m bytes from said public key certificate, wherein said at least a first byte c_1 is a binary representation of said number of bytes m in said public key certificate;

determining whether said binary representation of said number of bytes m in said at least a first byte c_1, is greater than the number of bytes of data in said digital signature data, n;

retrieving the remainder of said m bytes, if said determining step determines that said at least a first byte c_1 is greater than the number of bytes of data in said digital signature data, n; and,

applying said authentic public key to said digital signature data in order to verify said at least one of said first and second digital signatures.

129. (NEW) The authenticating method of claim 128, wherein said public key certificate parsing substep includes the further substeps of:

retrieving public key validity date data from said public key certificate;

determining if said public key validity date data is within an accepted date range; and,

validating said public key certificate with said public key validity date data, if said public key validity date data is within said accepted date range.

130. (NEW) The authenticating method of claim 129, wherein said public key certificate parsing substep includes the further substep of:

issuing an alert if said public key validity date data is not within an accepted date range.

131. (NEW) The authenticating method of claim 130, wherein said public key certificate parsing substep includes the further substeps of:

deciding whether to validate said public key certificate if said public key validity date data is not within an accepted date range, by checking guidelines issued by said third party.

132. (NEW) The authenticating method of claim 130, wherein said public key certificate parsing substep includes the further substeps of:

deciding whether to validate said public key certificate if said public key validity date data is not within an accepted date range, by consulting a public key certificate database.

133. (NEW) The authenticating method of claim 121, further comprising the step of :

presenting said self-authenticating document by an owner of said self-authenticating document to a commercial entity for authentication, wherein said presenting step is carried out prior to said machine-readable data processing step.

134. (NEW) The authenticating method of claim 133, wherein said authentic PIN-determining step further includes the substep of:

determining whether an owner of said self-authenticating document is available to input said authentic PIN, wherein said PIN-availability step determines that said authentic PIN is not available if said owner of said self-authenticating document is not available.

135. (NEW) A system for reading a self-authenticating document having machine-readable data including critical document data, digital signature data and a public key certificate, the system comprising:

personal identification means for receiving a personal identification number (PIN) from a presenter of said self-authenticating document; and,

image scanning and processing means for reading said self-authenticating document and retrieving said machine-readable data from said self-authenticating document, and for assembling an authenticatable data string from said critical document data and said received PIN;

parsing means for parsing said machine readable data to obtain said digital signature data and said public key certificate; and,

validating means for certifying said public key certificate to obtain an authentic public key, and for applying said authentic public key to said digital signature data for validating said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

136. (NEW) The system of claim 135, wherein said machine-readable critical document data includes data stored in a first and second format on said self-authenticating document, and wherein said image scanning and processing means comprises:

a first machine-readable data reading system for reading said critical document data stored in a first format from said self-authenticating document; and,

a second machine-readable data reading system for reading said critical document data stored in a second format from said self-authenticating document; and,

137
~~136.~~ (NEW) The system of claim 136, wherein said first format is magnetic ink character recognition (MICR) code, and said second format is bar code, and wherein said first machine-readable data reading system reading system is a MICR reader, and said first machine-readable data reading system reading system is a bar code reader.

138
~~137.~~ (NEW) The system of claim 135, wherein said machine-readable critical document data is stored in a bar code format on said self-authenticating document, and wherein said image scanning and processing means includes a bar code reading system for reading said bar code format to retrieve said critical document data.

139
~~138.~~ (NEW) The system of claim 135, wherein said validating means comprises:

a certification validation subsystem for validating said public key certificate with a third party public key and for obtaining said authentic public key; and,

a digital signature validation subsystem for validating said digital signature data with said authentic public key.

140
~~139.~~ (NEW) A system for reading a self-authenticating document, said self-authenticating document having machine-readable data including first critical document data stored on a magnetic ink character recognition (MICR) line, and first and second digital signatures, and a public key certificate stored on a bar code line, the system comprising:

a personal identification subsystem for receiving a personal identification number (PIN) from a presenter of said self-authenticating document; and,

an image scanner and processor system for reading said self-authenticating document and retrieving said machine readable data from said self-authenticating document, and for assembling an authenticatable data string from said first critical document data and said received PIN, said image scanner and processor including:

a magnetic ink character recognition (MICR) reader subsystem for retrieving said first critical document data from said MICR line;

a bar code reader subsystem for retrieving said first and second digital signatures and said public key certificate stored on a bar code line;

a parsing subsystem for parsing said bar code to obtain said first and second digital signatures and said public key certificate; and,

a validating subsystem for certifying said public key certificate to obtain an authentic public key and for applying said authentic public key to at least said second digital signature for validating said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

141
~~140.~~ (NEW) The system of claim 139, wherein said machine-readable data further includes second critical document data stored in said bar code line, wherein said bar code reader subsystem further retrieves said second critical